

Cyberbullying in Malaysia

Nov 2018

PRELIMINARY QUALITATIVE REPORT

PREPARED BY:

nerrativ

In collaboration with



A P U
ASIA PACIFIC UNIVERSITY
OF TECHNOLOGY & INNOVATION

Foreword

Cyberbullying: A hidden and growing problem in Malaysia

Platforms such as Facebook, Youtube, Whatsapp and Snapchat are the engine of human's life. Malaysians are fans of such platforms too, including youngsters who often use these platforms, without diligent monitoring and supervision.

While social media presents various benefits to its users, it also foster negative activities, including cyberbullying .

The issue of cyberbullying in Malaysia has been in the limelight since the last decade, and is prevalent in younger generations. This presents the risk of moral degradation amongst Malaysians, and importantly, loss of life.

It is imperative that cyberbullying is evaluated, analysed and understood with a view of reducing, preventing and mitigating such a negative behaviour from spreading, in a cancerous form.

What is Cyberbullying	4
Types of Cyberbullying	5
Cyberbullying in Malaysia	6
Cyberbullying Laws	9
Current Problems	10
Potential Solutions	12
References	13

What is Cyberbullying?

Cyberbullying was recognised as a real social problem when the word was recorded in the Oxford Dictionary in 2011.

Traditional approach of bullying seem to have evolved with the advent of affordable personal computers. Victims, often youngsters, are now subjected to “cyberbullying” by online communities. The anonymity provided by online platforms, including social media channels, present users the perfect cover to harass or intimidate others without repercussion of any sort. The evolution of technology has provided bullies with greater access to victims ¹.

Various definitions tried to encapsulate this multifaceted evolving occurrence. In general, cyberbullying is recognised as an act of bullying carried out using a digital communication device i.e. a computer or a mobile device ². It is usually an intentional act or series of acts carried out by a group or individual, often repeatedly and over time against victims who may not be able to defend themselves ³.

The increased usage of social media and messaging platforms, infer that cyberbullying can occur anywhere and at any time. This opens avenues for bullies to target individuals with less effort on the part of the bully ⁴.

Beyond a basic definition, there is no consensus on the scope of cyberbullying in Malaysia. For example, within a single legal jurisdiction, there seems to be different segmentation on the age limit of society affected by cyberbullying. Some limit the scope to children below the age of 18, while others include adults within the mix ⁵. Clearly there is a need to establish a Malaysian standard to provide clarity to the public.

Defining the scope becomes infinitely more complex when segmenting the issue into criminal and non-criminal types of cyberbullying which is jurisdiction sensitive.

In respect of the categories or types of cyberbullying, the list is non-exhaustive due to the ever-evolving nature of cyberspace. However, is still however necessary to understand key types occurring in Malaysia some of which are listed here:-

Types of Cyberbullying

Harassment

a sustained, constant and intentional form of bullying comprising abusive or threatening messages sent to the recipient or to a group.

Outing

A deliberate act to embarrass or publicly humiliate the victim or a group through the online posting of sensitive, private or embarrassing information without their consent.

Fraping

Logging into the victim's social networking account and impersonating the victim by posting inappropriate content in their name.

Flaming

starting a form of online fight.

Impersonation

Pretending to be someone else and sending or posting material to get that person in trouble or danger or to damage that person's reputation or friendships (similar to Fraping).

Exclusion

The deliberate act of leaving someone out.

Trolling

The deliberate act of provoking a response through the use of insults or bad language on online forums and social networking sites.

Cyberstalking

Making real threats to the victim's physical wellbeing and/or safety.

Trickery

Similar to outing where the cyberbully reveals sensitive or embarrassing information publicly online except that in the case of trickery, information is obtained by deception.

Denigration

sending or posting gossip to ruin someone's reputation.

Cyberbullying in Malaysia

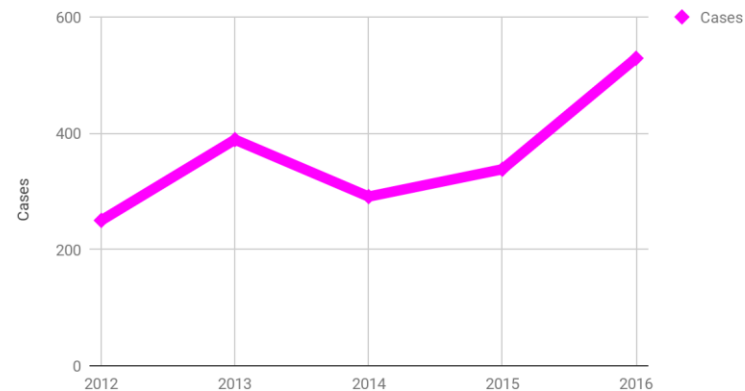
Following similar international trends, Malaysia's (reported) cyberbullying rate has generally been on a rising trend⁶. Statistics suggest that the primary demographic for victims being between 13 to 15 years of age⁷.

According to an international survey by Ipsos, which focused on parents and individuals between the ages of 16 to 64, it was found that awareness of cyberbullying in Malaysia is quite high (85%)⁸.

Approximately 1 in 4 Malaysian parents indicated that their child has experienced some form of cyberbullying.

Malaysia has been ranked 6th amongst 28 countries surveyed in the category of parents reporting their child having been a victim of cyberbullying.

Cases reported to CyberSAFE



What is the impact of cyberbullying?

Worldwide, cases of cyberbullying have resulted in a range of outcomes. At the mild end of the spectrum is anger and being upset. As the severity of cyberbullying intensifies victims have succumbed to depression, anxiety and in severe cases, suicide.

If not discovered or addressed adequately, cyberbullying may evolve in its methodology and impact. A simple online troll can quickly cross the line and become an act of harassment. In many cases, despite knowing that their actions are wrong, many youngsters may not realise the severity of their online actions.

To date, no comprehensive study has been done on the impact of cyberbullying in Malaysia, and with the increasing volume of cases, it would seem necessary to address this concern.

The CyberSAFE in Schools Reports

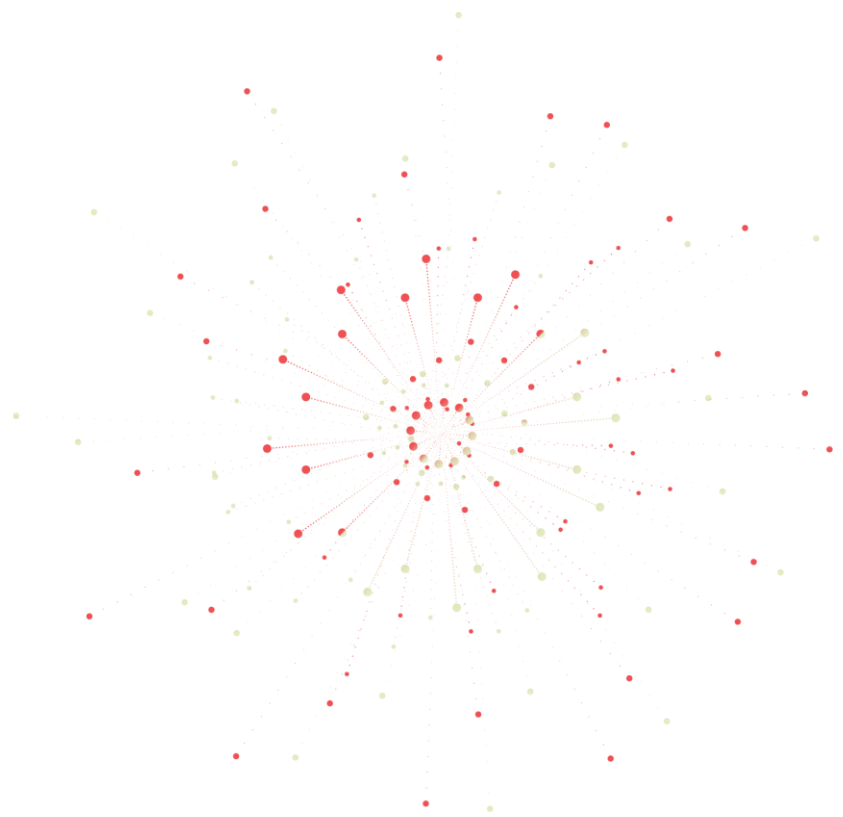
The CyberSAFE in Schools surveys have generated considerable insight into cyberbullying among schoolgoing children within the ages of 7-19⁹.

With a good representation of 14,000 to 18,000 students, the survey's outcome have generated a deserving attention.

The 2014 survey found that 26% of all participating schoolchildren have reported being bullied online. Nearly 70% them indicated bullying in terms of calling of mean names, posting improper messages and inappropriate photos sharing.

It is noteworthy to observe Malaysians lack a clear understanding of what constitute cyberbullying. An average of 64% of those surveyed considered sending improper SMSes, posting inappropriate photos, and pretending to be someone else is not cyberbullying.

The 2015 report suggested that there were low likelihoods of children experiencing cyberbullying which contradicts the Ipsos's 2014 report.



Some key findings of the CyberSAFE in Schools reports

- 40% of school children do not know how to protect themselves online;
- 83% of school children are vulnerable to online risks due to minimal protective actions taken;
- Two-thirds of young school children (below 13 years old) take very low protective steps (zero to three) towards online safety. However, 52% of these school children still believe that they are safe online;
- An average 70% of school children are not concerned with the invasion of their privacy or the anonymity of the person they interact with;
- There is no indication that children from urban areas take a higher level of protective action as compared with those in rural areas;
- The level of awareness does not necessarily translate to positive action. More than 40% of children who said that online safety is important, continue to exercise low levels of online protection;
- 50% of children are unsupervised when online, with close to 40% claiming they are not bound by any rules on safety;
- 61% of the children tend to turn to their family members when encountering negative online experiences;
- Although there are 10 reporting-channel options, there are still 6% of schoolchildren who chose to remain silent;
- Families with computers in common areas of their home tend to exert more rules on cybersafety. However, this measure alone is insufficient, as an increasing number of children are accessing the internet on their mobile phones.

Cyberbullying Laws

Malaysia does not have a dedicated cyberbullying law. For an offence of cyberbullying to be prosecuted, it must fall under either the Penal Code or the Communications and Multimedia Act 1998 (CMA)¹⁰.

The Penal Code captures such offences as ‘criminal intimidation’¹¹ or ‘criminal intimidation by anonymous intimidation’¹². It must be noted that prosecution under the Penal Code makes the offence criminal in nature meaning that the standard of proof and evidence can be very high.

Due to the definitions provided by these sections, a number of types and severity of cyberbullying cases may be excluded from prosecution despite having a negative impact on the victim.

If a case cannot be prosecuted under the Penal Code it is likely to be captured under the CMA. Section 223 of the act is wide enough to capture most cyberbullying offences as it includes obscene, indecent, false, menacing or offensive in character with intent to annoy, abuse, threaten or harass another person. The act goes further to place a duty on the network providers to prevent offences such as cyberbullying.¹³ Under the CMA the Malaysian Commission of Multimedia and Communications (MCMC) is granted significant investigative and prosecutorial powers, some equivalent to the police¹⁴. It is therefore arguable that significant reduction in cyberbullying trends may be seen by increased enforcement of the existing provisions of law.

A more detailed examination of the law with comparative analysis is provided at **Annexure A**.

Current Problems

Despite increased efforts to combat the rise of cyberbullying occurrence, many countries are beginning to reassess the solutions being explored.

In Malaysia we have identified 3 key areas that may benefit from reassessment, namely:-

- Deeper understanding of Cyberbullying;
- Structured Reporting;
- Analysis of Reporting Data

Deeper Understanding of Cyberbullying

The rising number of cyberbullying cases nationally could be attributed to a plethora of factors. However one factor that stand out is the scope of existing awareness.

It would seem that the high level of awareness is centered around the existence of cyberbullying as an issue. However most stakeholders rarely have information on key areas i.e.:-

- Understanding on the types of cyberbullying;
- Symptoms to look out for to identify if a person may be either a victim or a bully;
- Lines of action to take when someone is suspected as either a victim or a bully

More importantly, even where information is available on certain online platforms, there is limited depth to such information ¹⁵. Consequently parents, guardians, teachers and even victims themselves are limited in their understanding of the subject.

Taking lessons from abroad, we find dedicated sites for reporting and awareness to which other similar intentioned sites point towards. Examples are:

- <https://www.stopbullying.gov/cyberbullying/how-to-report/index.html> (USA)
- <https://www.esafety.gov.au/reportcyberbullying> (Australia)
- <https://www.bullying.co.uk/cyberbullying> (UK)

Data Availability & Analysis

Other than the CyberSAFE reports cited earlier, there are limited studies carried out into the various facets of this issue.

Cyberbullying reporting has been limited to a particular entity i.e. Cybersecurity Malaysia, MCMC. Consequently this leads to an inability of different stakeholders to focus on the appropriate solution to the variety of problems faced due to cyberbullying.

Further, there seems to be no published reports on the analysis of data collected by way of case reports.

In terms of analysis, the field could benefit from a more data driven analysis.

Reporting

On this issue we note that the MCMC page on cyberbullying provides a very clear outline of processes upon a complaint being received. However the reporting portals of MCMC, Communications and Multimedia Content Forum of Malaysia (CMCF) and CyberSAFE are not dedicated cyberbullying reporting portals. Each one seem to be overlapping with different issues and content. As cyberbullying can involve elements of fear and embarrassment, we opine that the reporting portal must be structured and guided to allow for an easier reporting process.

Potential Solutions

Awareness

In order to provide the general public with a comprehensive understanding of cyberbullying and the variety of components affecting it, i.e. psychological impacts and rehabilitation avenues, education for perpetrators (particularly children) there should be an online platform that consolidates all information including types of cyberbullying, available agencies to contact and any important, detailed information that both youth and adults should be aware of.

Both adults and their corresponding youth must work hand in hand to ensure a mutual understanding on how the Internet works and the dangers lurk within it. Since the new generations are the frequent users of the Internet, it follows that they are more aware of the use, the tools and the features of the internet than the older generations ¹⁶.

Reporting

To compliment the awareness solution, a consolidated structured and guided reporting platform should be developed. The structure of this platform should be geared to handhold a user through the process while collecting critical information including evidence.

Similar to the current MCMC reporting process, an individual reporting must receive notifications on the status of the case. The portal may (through a weightage assessment procedure), direct the complaint to the appropriate entity for further action.

Data Analysis

As a final but most important feature is analysis of the data collected through the reporting system. Using data science methodologies, actionable insights should be generated to allow for the relevant agencies to take the appropriate action.

- 1 <https://www.bark.us/blog/the-history-of-cyberbullying/>
2. <https://en.oxforddictionaries.com/definition/cyberbullying>
3. Smith, P. K., Mahdavi, J., Carvalho, M., Fisher, S., Russell, S., & Tippett, N. (2008). Cyberbullying: Its nature and impact in secondary school students. *Journal of Child Psychology and Psychiatry, and Allied Disciplines*
4. Garinger, H. M. (2008). Cyber pox: A look at female adolescent cyberbullying. *Michigan Journal of Counseling*
- 5 <https://www.thestar.com.my/news/nation/2018/04/18/celebs-stand-up-against-cyberbullying-and-fake-news/>
6. <https://www.comparitech.com/internet-providers/cyberbullying-statistics/>
7. https://digi.cybersafe.my/files/article/CyberSAFE_Survey_Report_2014.pdf
8. <https://www.ipsos.com/en/global-views-cyberbullying>
9. https://digi.cybersafe.my/files/article/CyberSAFE_Survey_Report_2014.pdf
10. Certain specific cyberbullying acts i.e. fraping or those that are sexual predatory in nature may attract other legislation i.e. Evidence Act 1950, Sexual Offences Act Against Children Act 2017.
11. Section 503, Penal Code
12. Section 507, Penal Code
13. Section 263, CMA 1998
14. Section 246, CMA 1998
- 15 CyberSAFE website
16. https://www.academia.edu/28965543/Level_of_Cyberbullying_among_Malaysian_Children_Some_Empirical_Evidence

About this Research

This study was conducted as preliminary research into the issue of cyberbullying with the aim of solution building. Naturally there are numerous aspects of the issue that require more in depth research and subject to availability of data this project intends to undertake such research. For this purpose the team will look to expand its pool of expertise through collaboration with domain experts and other interested parties.

Asia Pacific University (APU) Research Team

We thank the team of collaborators from APU that undertook the valuable initial research of this paper, namely Associate Professor Dr Mudiaran Kuppusamy, Janice Leong Ching Lai, Sushant Patkar and Swami Pankaj.

Expert Collaborators

We extend a special thanks to the sole expert collaborator on this paper, Dr Jaspal Kaur Sadhu Singh, who provided direction, advice and research specifically on the area of the legal framework surrounding the issue.

About Narrativ

Narrativ brings a new dimension to the field of social impact by executing CSR Data projects which are aimed towards achieving long-term change. These projects are data driven with a key focus on components of awareness and technological solutions executed through collaboration with project partners and collaborators.

Annexure A

A Review of the Regulatory Response to Cyberbullying

By Dr Jaspal Kaur Sadhu Singh

Definition of bullying: Legal nomenclature

With most criminal acts, the definition or elements of the criminal acts must be clearly set out. It has to be liberally permissive, to include or adapt to include, a wide range of acts but circumscribed adequately to capture the unique characteristics of the phenomenon presenting the mischief to the law.

A good reference point on definitional aspects of the phenomenon is the position taken in the US. Anti-bullying laws vary from state to state. These laws list the specific behaviours that constitute bullying which can include teasing, threats, intimidation, stalking, harassment, physical violence, theft, and public humiliation. The reference to the nomenclature “cyberbullying” is used when bullying takes place through the medium of information and communication technology and devices.

Several state laws, such as in Arizona, delegates definitional responsibility to the school districts to define the specific actions that constitute bullying. This allows the various school districts to develop a soft law around bullying which will enable the ease of adaptability and change.

State laws such as those enacted in California, Connecticut and Illinois, to name a few, define bullying, but fall short of specifying bullying through electronic communication.

In California, the law defines bullying as any physical or verbal conduct, including written communications, that may cause fear, mental distress, or interference with the victim's studies.

In Connecticut, it is defined as written, oral or physical acts directed at another student within the same school district that cause physical or emotional harm, cause fear, or creates a hostile learning environment. In Illinois, bullying is defined as "any severe or pervasive" act that could cause fear of harm, a detrimental physical or mental health effect, or interference with the victim's academic performance or extracurricular activities.

In New Jersey, bullying is defined as any gesture or any physical, verbal or written act that is motivated by the actual or perceived traits of the victim. The bullying statute covers school functions, as well as activities off campus and on school buses.

In New York, it is defined as threats, intimidation or abuse that unreasonably and substantially interferes with the victim's educational performance, opportunities, or mental, physical or emotional health. Bullying can apply even if it occurs off school property, so long as it would create a foreseeable risk that the bullying acts might reach school property.

According to the law in Texas, bullying is defined as any written, verbal or physical act that physically harms a student or damages a student's property, or that creates an intimidating, threatening or abusive educational environment.

In Virginia, bullying is any aggressive or unwanted behaviour that is intended to harm, intimidate, or humiliate the victim. Bullying must also involve a real or perceived imbalance of power between the bully and the victim, and it must either be repeated over time or cause severe emotional trauma. Virginia explicitly states that "ordinary teasing, horseplay, argument, or peer conflict" do not count as bullying.

However, the state law in Washington, is one of the few that clearly includes the medium of bullying to extend to include the "electronic" medium. Washington defines bullying as any intentional electronic, written, verbal or physical act that physically harms a student or damages the student's property, interferes with the student's education, creates an intimidating or threatening education environment, or substantially disrupts the orderly operation of the school.

Regulatory Framework adopted

a. US

In the US, it is evident from the section above that the state laws are varied in their approach. Essentially there are three:

- i. Where the schools are given the statutory authority to regulate bullying by adopting procedures and penalties workable to their school;
- ii. Where the legislation clearly creates an offence of bullying and is viewed as an offence. However, there is no specific mention of its extension to cyberbullying; and finally,
- iii. Similar to (ii) above but with clear inclusion of the medium of bullying to include “electronic” communication as a medium of the bullying.

a. UK

In the UK, the relevant legislation is the Education and Inspections Act 2006. Part 7 which is titled ‘Discipline, behaviour and exclusion’ and specifically Chapter 1 titled ‘School Discipline’ of the said chapter provides guidance on how schools should approach the problem of bullying. Section 88 of the 2006 Act mandates that the governing body of the school must ensure that policies designed to promote good behaviour and discipline on the part of its pupils are pursued at the school. Section 89(1) requires the head teacher of the school to determine a behaviour policy. Although the provision of establishing a behaviour policy does not make specific mention but its scope is wide enough to include bullying or cyberbullying. The subsection reads:

The head teacher of a relevant school must determine measures to be taken with a view to -

- (a) promoting, among pupils, self-discipline and proper regard for authority,
- (b) encouraging good behaviour and respect for others on the part of pupils and, in particular, preventing all forms of bullying among pupils,
- (c) securing that the standard of behaviour of pupils is acceptable,
- (d) securing that pupils complete any tasks reasonably assigned to them in connection with their education, and
- (e) otherwise regulating the conduct of pupils.

Although there are no specific laws on bullying, similar to the position in Malaysia, harassing or threatening behaviour or communications could fall within the ambit of a criminal offence. The legislation which provides for such crimes include the Protection from Harassment Act 1997, the Malicious Communications Act 1988, the Communications Act 2003, and the Public Order Act 1986.

School staff members are also accorded clear legislative powers under section 2 of the Education Act 2011 to search pupils. These powers allow school staff members to tackle cyber-bullying by providing a specific power to search for and, if necessary, delete inappropriate images or files on electronic devices, including mobile phones. These powers also include the power to seize to facilitate the offences set out in the criminal provisions above.

The legal landscape in Malaysia

There were news reports in 2017 where the then Deputy Minister had stated that a law on cyberbullying was being drafted. To date, there have been no legislative initiatives. There is no *lex specialis* dealing with bullying or cyberbullying.

a. The Penal Code

Reliance on traditional criminal laws found in the Penal Code would include the offence of 'Criminal Intimidation' under section 503, which provides:

Whoever threatens another with any injury to his person, reputation or property, or to the person or reputation of any one in whom that person is interested, with intent to cause alarm to that person, or to cause that person to do any act which he is not legally bound to do, or to omit to do any act which that person is legally entitled to do, as the means of avoiding the execution of such threat, commits criminal intimidation.

For the offence of 'Criminal intimidation by an anonymous communication', section 507 of the Penal Code provides:

Whoever commits the offence of criminal intimidation by an anonymous communication, or by having taken precautions to conceal the name or abode of the person from whom the threat comes, shall be punished with imprisonment for a term which may extend to two years, in addition to the punishment provided for the offence by section 506.

a. Communications and Multimedia Act 1998

In terms of a *lex specialis*, the legislation that deals with electronic communication is the Communication and Multimedia Act 1998. A possible provision that could deal with cyberbullying is section 223 of the Act when the medium to commit the offence is the use of any online facility. In sub-section (1) to section 233, it is provided that:

¹ 'Chong: Laws on cyber bullying being drafted' (The Star Online, 7 February 2017) <<https://www.thestar.com.my/news/nation/2017/02/07/chong-laws-on-cyber-bullying-being-drafted-such-harassment-can-affect-students-badly/#60vT4WIKVkJZpxkl.99>>; 'Education Ministry to draft cyberbullying laws' (The Malay Mail, 7 February 2017) <<https://www.malaymail.com/s/1309045/education-ministry-to-draft-cyberbullying-laws>>.

² Punishment for section 503 is provided for under section 506 which provides:
Whoever commits the offence of criminal intimidation shall be punished with imprisonment for a term which may extend to two years or with fine or with both; if the threat is to cause death or grievous hurt, or to cause the destruction of any property by fire, or to cause an offence punishable with death or imprisonment, or with imprisonment for a term which may extend to seven years, or to impute unchastity to a woman, shall be punished with imprisonment for a term which may extend to seven years or with fine or with both.

A person who by means of any network facilities or network service or applications service knowingly –

- (i) makes, creates or solicits; and
- (ii) initiates the transmission of, any comment, request, suggestion or other communication which is obscene, indecent, false, menacing or offensive in character with intent to annoy, abuse, threaten or harass another person;

The 1998 Act may even be utilised to extend the responsibility of dealing with cyberbullying to social media platforms. Section 211 under the heading ‘Prohibition on provision of offensive content’ in sub-section (1) provides that:

No content applications service provider, or other person using a content applications service, shall provide content which is indecent, obscene, false, menacing, or offensive in character with intent to annoy, abuse, threaten or harass any person.

Note that Section 6 of the Communications and Multimedia Act 1998 defines “content application service” as “application service which provides content”.

Further, section 263 imposes a general duty on licensees. The section reads;

- (1) A licensee shall use his best endeavour to prevent the network facilities that he owns or provides or the network service, applications service or content applications service that he provides from being used in, or in relation to, the commission of any offence under any law of Malaysia.
- (2) A licensee shall, upon written request by the Commission or any other authority, assist the Commission or other authority as far as reasonably necessary in preventing the commission or attempted commission of an offence under any written law of Malaysia or otherwise in enforcing the laws of Malaysia, including, but not limited to, the protection of the public revenue and preservation of national security.

Opinion

There needs to be a dialogue on the right regulatory model to approach the problem of cyberbullying. With all regulatory frameworks, a definition of the nature of the criminal behaviour to be regulated requires a study of the phenomenon that leads to the said criminal behaviour. A study of cyberbullying complaints will require an exercise of content analysis identifying common themes in order to set out the parameters of the act requiring regulation.